Datenschutz und hippokratischer Eid

Auswirkungen der **EU-DSGVO** auf Augenarztpraxen und Augenzentren

BONN-BAD GODESBERG/HOFGEISMAR Es ist teilweise in Vergessenheit geraten, dass Datenschutz bereits im Eid des Hippokrates verwurzelt ist: „Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten." Dem gegenüber ist die EU-Datenschutzgrundverordnung (EU-DSGVO) derzeit in aller Munde. Teilweise werden die Bußgelder bei Datenschutzverstößen, die bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes erreichen können, in den Vordergrund gestellt.


Haupt

Thomas Haupt


Moers

Stephan Moers

Datenschutz ist nichts Neues, denn der deutsche Vorläufer der EU-DSGVO – das Bundesdatenschutzgesetz (BDSG) – existiert bereits seit 1977. Das BDSG regelt unter anderem, wie personenbezogene Daten zu verarbeiten sind:

• Personenbezogene Daten müssen zulässig, nachvollziehbar für den Betroffenen für festgelegte Zwecke und in für den Zweck angemessener Weise verarbeitet werden.

• Sie müssen sachlich richtig verarbeitet werden, erforderlichenfalls gelöscht und berichtigt werden können und dürfen nur so lange gespeichert werden, wie es für die Zwecke erforderlich ist.

• Die Sicherheit der Daten ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten.

Um die genannten Punkte in Augenarztpraxen und Augenzentren umzusetzen, bedarf es bestimmter organisatorischer Regelungen und angemessener Sicherheitsmaßnahmen. Die wichtigsten sind:

• Vorhandensein von Informationen zum Umgang mit personenbezogenen Daten für Patienten und Mitarbeiter,

• Dokumentation von Datenverarbeitungsverfahren und

• Abschluss von Verträgen mit zuliefernden Unternehmen, sofern personenbezogene Daten verarbeitet werden.

Diese vor dem Hintergrund des BDSG getroffenen Regelungen sind nun im Sinne der EU-DSGVO fortzuschreiben. Was viele nicht wissen: Die EU-DSGVO ist bereits am 25. Mai 2016 in Kraft getreten. Zur Anwendung kommt sie erst nach einer Übergangsfrist von zwei Jahren, somit ab dem 25. Mai 2018. Sie gilt direkt und bedarf keines nationalen Umsetzungsgesetzes. Gleichzeitig gilt das neue Bundesdatenschutzgesetz (BDSG) 2018, das die EU-DSGVO zum Teil konkretisiert. Beim Wechsel vom BDSG zur EU-DSGVO sind zwei Aspekte hervorzuheben:

1. Bislang wurde das BDSG durch Spezialgesetze verdrängt. Diese Subsidiarität fällt weg. Nationale Gesetze sind somit im Lichte der EU-DSGVO auszulegen.

2. Zweiter wichtiger Punkt ist die Einführung einer Datenschutz-Rechenschaftspflicht. Auf Anfrage von Betroffenen oder Behörden sind Ärzte und Zentren in der Pflicht, nachweisen zu können, dass sie die Grundsätze für die Verarbeitung personenbezogener Daten einhalten.

Was ist im Rahmen der EU-DSGVO zu tun? Konkret bedeutet das:

• Datenschutzmanagement: In den Augenarztpraxen und Augenzentren sind die Datenschutzpflichten durch ein Datenschutzmanagement zu konkretisieren. Die Mitarbeiter sind auf den konformen Umgang mit personenbezogenen Daten (einschl. Kenntnisnachweis) zu verpflichten.

• Sicherheit der Daten: Die Sicherheit der verwendeten Rechnersysteme und die Sicherheit der genutzten Services ist zu gewährleisten. Dies fängt bei Bildschirmsperren an und endet bei der baulichen Absicherung von Serverräumen.

• Informationspflicht: Patienten, Mitarbeiter und Dritte sind zum Zeitpunkt der Erhebung ihrer Daten zu informieren. Dies gilt auch für die Webseitenbesucher (vgl. Art. 13 EU-DSGVO).

• Weitergaben von Daten: Werden personenbezogene Daten übermittelt, ist dies durch Verträge schriftlich zu fixieren. Das gilt beispielsweise im Rahmen einer Auftragsverarbeitung durch externe Abrechnungsorganisationen, externe Lohnbuchhalter oder im Rahmen einer „Gemeinsamen Verantwortung" bei gemeinsamen Projekten mit anderen Einrichtungen.

• Datenschutzbeauftragter (DSB): Ein solcher muss in der Regel erst ab mindestens zehn Personen benannt werden, die regelmäßig Daten verarbeiten. Im medizinischen Umfeld kann eine Benennungspflicht aus Art. 37 Abs. 1 lit. c EU-DSGVO vorliegen, wonach bei umfangreicher Verarbeitung medizinischer Daten eine Bestellpflicht vorliegt. Umfangreich dürfte die Verarbeitung in jedem Fall in Augenkliniken und Medizinischen Versorgungszentren sein. Ein einzelner praktizierender Augenarzt wird in der Regel keinen DSB benennen müssen; hier können aber noch weitere Faktoren ins Gewicht fallen (siehe hierzu das Working Papier 248 der Artikel-29-Gruppe*). Die eigene Einschätzung sollte in jedem Fall gut begründet und dokumentiert werden – die Nichtdurchführung einer Datenschutzfolgenabschätzung oder Nichtbenennung eines DSB liegt im mittleren Bußgeldrahmen von zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes.

• Verzeichnis der Verarbeitungstätigkeiten: Über alle Verfahren, bei denen personenbezogene Daten verarbeitet werden, ist ein Verzeichnis zu führen. Hierin werden pro Verarbeitungstätigkeit die Angaben zum Verantwortlichen, die Verarbeitungszwecke, die Beschreibung von Kategorien betroffener Daten, Datenempfänger, Übermittlungen an eine internationale Organisation, Fristen für die Datenlöschung sowie Informationen zur Datensicherheit aufgeführt.

Zeitpunkt der Patienteninformation

Aus den oben genannten Punkten wird nachfolgend noch auf die Informationspflicht eingegangen. Denn hieraus ergibt sich nach Art. 12–14 EU-DSGVO Handlungsbedarf: Der Patient ist zum Zeitpunkt der Erhebung seiner Daten über die Pflichtangaben zu informieren. Das betrifft nicht nur die Datenschutzerklärungen für Webseitenbesucher, sondern auch die Terminvergabe am Telefon. Hinsichtlich der Umsetzung der Information am Telefon gab es mitunter kontroverse Diskussionen. Die Vorstellung, einem Erstpatienten, der lediglich einen Termin vereinbaren möchte, fünf Minuten lang Datenschutzerklärungen vorzulesen, erscheint geradezu grotesk. Auch eine Telefonschleife mit den nötigen Datenschutzerklärungen vor Durchstellung zur Terminvergabe erscheint wenig praktikabel. Bei der reinen Vergabe eines Termins ist ein Vorlesen einer Datenschutzerklärung mit einem unverhältnismäßig hohen Aufwand verbunden, weshalb nach Ansicht der Autoren hierauf verzichtet werden sollte. Hier hilft der Erwägungsgrund 62 der EU-DSGVO: Die Pflicht zur Information erübrigt sich, „wenn [...] die Unterrichtung der betroffenen Person [...] mit unverhältnismäßig hohem Aufwand verbunden ist". Es reicht somit aus, wenn die Datenschutzinformationen beim Erstbesuch dokumentiert übergeben werden. Der Patient muss nicht unterschreiben; ein Aushang reicht allerdings auch nicht aus. Es gibt bereits Behörden, die dieser Ansicht folgen.

Der Augenarzt muss nachweisen können, dass er die Pflichtinformationen zur Verfügung gestellt hat. Bei einer Terminvergabe über die Internetseite hingegen kann man leicht und nachweislich der Informationspflicht gerecht werden.

Fazit und Zusammenfassung

Die EU-DSGVO bringt nicht nur hohe Bußgelder bei Datenschutzverstößen mit sich, sondern auch eine Nachweispflicht. Augenarztpraxen und Augenzentren müssen belegen können, dass sie personenbezogene Daten ordnungsgemäß verarbeiten. Sofern noch nicht geschehen, sollte hiermit unmittelbar begonnen werden. Beispielhaft findet sich hier eine geeignete Vorlage: https://www.lda.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf

Und übrigens: Der mehr als 2000 Jahre alte hippokratische Eid wurde Ende 2017 überarbeitet. Die neue Version verpflichtet Ärzte, Wissen zum Wohl der Patienten mit Kollegen zu teilen. Umso wichtiger ist dabei, die Grundsätze des Datenschutzes einzuhalten. ■

* Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission, der zukünftige europäische Datenschutzausschuss. Er setzt sich aus den Aufsichtsbehörden der Mitgliedsstaaten zusammen. Die „Working Paper" der Gruppe geben Hilfestellung beim Verständnis der Regelungen.

Autoren:
Stephan Moers
Geschäftsführer | Datenschutzbeauftragter (GDDcert. EU)
Datenschutzberatung Moers GmbH
Neue Str. 22, 34369 Hofgeismar
Tel.: 05671-7492-491
E-Mail: sm@dsb-moers.de
Dr. Thomas Haupt
Kaufmännischer Leiter
Augenklinik Dardenne SE
Friedrich-Ebert-Str. 23–25
53177 Bonn-Bad Godesberg
Tel.: 0228-8303-115
E-Mail: haupt@dardenne.de